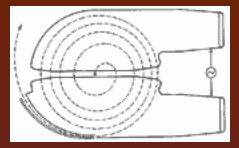
Speaking Safety

Safety Systems

USPAS

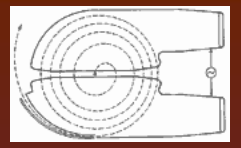
June 2004



Outline

- Overview of Safety
- Definitions

- Objective
  - Communicate the nomenclature and context for terms used in this class.

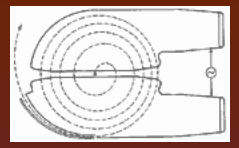


System Safety

What is System Safety?

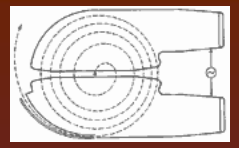
System safety is the practice of proactive hazard management.

It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from conception to decommissioning.



System Safety

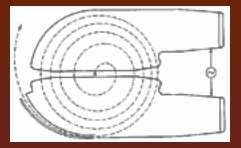
- System Safety is a holistic approach to critical systems' management.
- Safety related systems must be evaluated and designed in the context for which they are to be applied.
- This includes foreseeable changes and upgrades over the life of the system.



System Safety

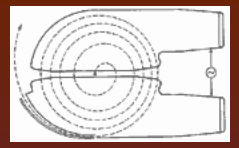
From N. Leveson, "Safeware"

- *System safety emphasizes building in safety, not adding it to a completed design.*
- *System safety deals with systems as a whole rather than with subsystems or components.*
- *System safety takes a larger view of hazards than just failures.*
- *System safety emphasizes analysis rather than past experience or standards.*
- *System safety emphasizes qualitative rather than quantitative approaches.*
- *System safety recognizes the importance of tradeoffs and conflicts in system design.*
- *System safety is more than just system engineering*



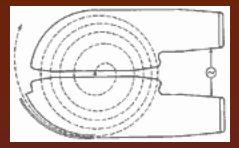
Systems Safety

- Original safety models used the fail and fix method.
- Design a product to the best practices (usually over design), wait until it fails, fix the cause of the failure, and continue.
- Quite often ‘improvements’ were introduced that made the actual incremental improvement questionable.
- Coupled with this was an acceptance of some accidents as inevitable. In addition, the consequence of accidents involved a few individuals at most.



System Safety

- Greater consequences from failure.
  - Technology allows concentration of great amounts of energy in small areas. This energy, if not controlled, can lead to more catastrophic accidents.
- Greater dissemination of information
  - People saw pictures of the Hiroshima, Nagasaki atomic bombs, Apollo 1 fire, Bhopal…etc.
  - Intolerance for poor living and working conditions at the beginning of 20th century eventually spilled over into intolerance for being placed in danger in the name of "progress".



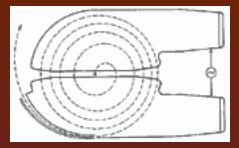
What is a Safety System?

A Safety System is an engineered system that reduces the risk of harm to people, equipment, or the environment that may arise from the operation of a process or equipment.

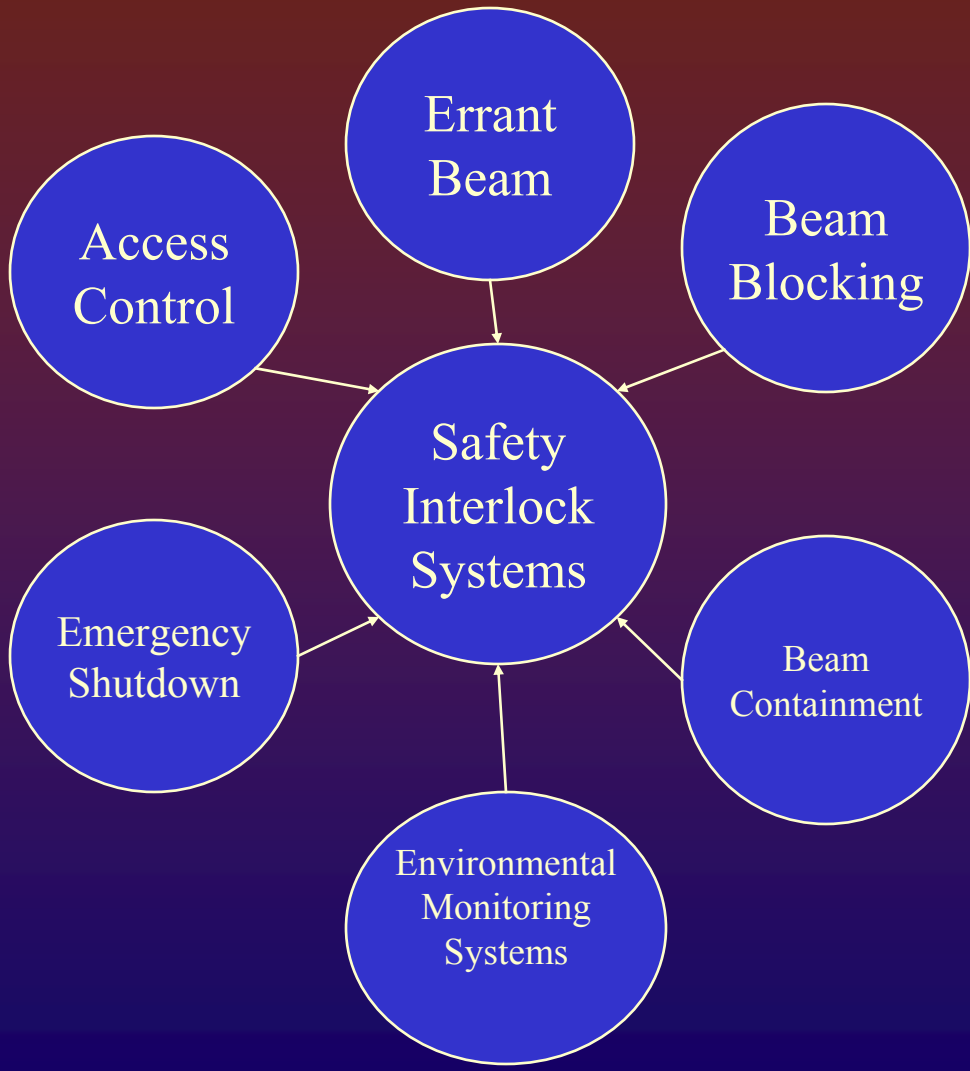
General Attributes of a Safety System:

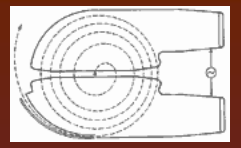
- Autonomous – acts on it's own to achieve a safe state
- Requires kinetic energy external to the process (although fails-safe)
- Sensor $\Rightarrow$ Logic $\Rightarrow$ Final Control Element
- Independently verifiable safety function

What is a Safety System for Accelerators?



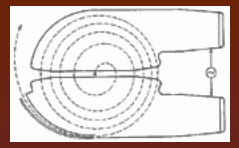
- Typical elements
  - Access Control
  - Safety Interlock Systems
  - Emergency shut down systems
  - Errant beam detection
  - Beam Containment
  - Environmental monitoring systems
    - Radiation monitoring
    - Oxygen monitoring
    - Chemical agent monitoring
    - Explosive gas monitoring
    - Laser/RF Monitoring





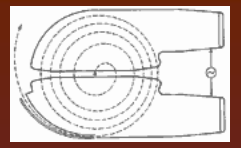
Harm

- Damage to people, the environment, or property.
  - Intentional
  - Accidental
  - Negligent



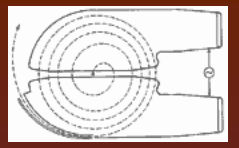
Safety

- Freedom from harm or potential harm



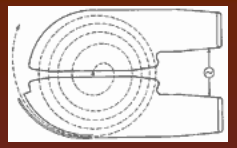
Accident/Mishap

- An event that results in a definable level of harm or loss.
  - Minor
  - Severe
  - Catastrophic
- Due to an unmitigated release of hazardous energy.
- Requires both uncontrolled energy and exposure to the harmful effects of the energy.



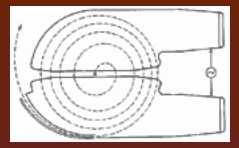
Hazard

- A state or set of conditions of a system within a given environment that will lead to an accident.
- Usually involves potential energy.



Risk

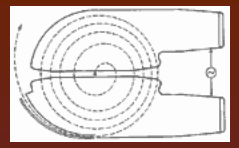
- A measure of the combination of hazard severity, likelihood, exposure, and opportunity that could lead to an accident.



Concrete Risk

- Risk of harm to people
- Risk of harm to the environment
- Risk of harm to equipment

Objective vs. Perceived Risk (especially radiation)



What weight has perception?

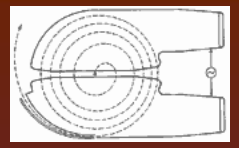
Most individual risks feed into a larger concern …

Q.) Where does perception have an impact?

A.) Institutional risk.

Perceived Risk

Sometimes Perceived Risk is the dominating factor in a risk assessment

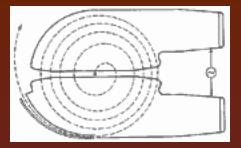


Esoteric Risk

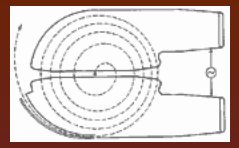
Schedule Risk

Institutional Risk

- Risk to mission
- Risk of public perception

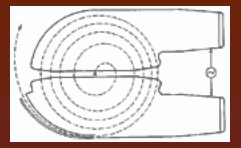


For practical purposes most risk can be associated with institutional risk. Therefore management is ultimately responsible for making an informed decision about how much risk they are willing to accept.



Approaches to safety system risk management

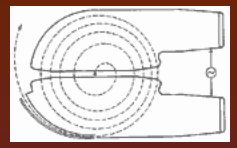
- **ALARP**
- **System Safety (e.g. MIL 882D)**
- **Regulation**
- **SIL**



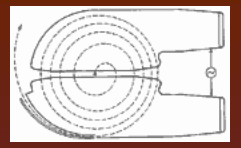
Risk Reduction

The purpose of safety programs is to identify risk and design methods to reduce the risk to the acceptable region over the life of the facility or system.

Methods of Mitigation



- Risk Assessment
  - Mitigation Required?
    - Engineering Controls
      - Eliminate
        - Process Change
        - Substitution
      - Reduce
        - Dilution/ Ventilation
        - Isolate
          - Active
            - Limit/ Remove
              - Access Control
              - Safety Interlock
              - Detection/ Monitoring
          - Passive
            - Shield
            - Distance
            - Enclose
      - Alarm/ Warn
    - Administrative Controls
      - Time/ Exposure
      - Training
      - Procedure
    - Personal Protective Equipment (PPE)

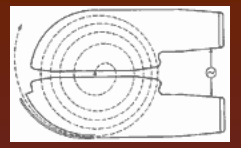


Reliability

The probability that a piece of equipment will perform it's intended function satisfactorily for a prescribed time and under stipulated environmental conditions.

Elements of reliability:

- Equipment
  - The thing that enables a hazard to occur
- Probability
  - Equipment will eventually fail, it's a matter of how and when
- Time
  - When
- Environment
  - Assumptions as to the operating conditions of the equipment

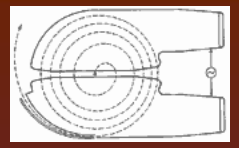


Reliability

Safety Reliability - The probability that a piece of equipment will perform the intended safety function over a given time period.

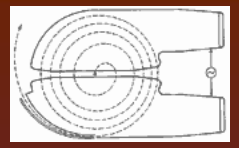
Safety Availability – the probability that a piece of equipment is able to perform the intended safety function when the hazard can be present.

$$SA = 1 - PFD$$



Safety Integrity Level

- Applies a range to the average probability of fail dangerously (PFD_{avg}) of a safety instrumented function.
- Each level covers 2 orders of magnitude



DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	**Average Probability of Failure on Demand**	**Risk Reduction**
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to $\leq$ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to $\leq$ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to $\leq$ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to $\leq$ 100

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	**Frequency of Dangerous Failures Per Hour**
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$